ihcda

Indiana Housing & Community Development Authority

Homeless Management Information System Policies and Standard Operating Procedures

Spring, 2010

Table of Contents

In 2004 the US Department of Housing and Urban Development (HUD) published the draft data standards for Homeless Management Information Systems (HMIS). These standards defined the data elements and formats through which all HUD McKinney-Vento Program funded projects were to report. In Indiana, a statewide coalition consisting of homeless providers and local Continuums of Care was established to review and select a software vendor for the Indiana Balance of State HMIS. After review, the Affordable Wide Area Relational Data System (AWARDS) from Foothold Technology, Inc. was selected. This is a web based software requiring only internet access for use. The HMIS was initially separately administered for South Bend, Evansville and the Indiana Balance of State (89 of the 92 counties in Indiana) by the Indiana Coalition on Housing and Homeless Issues (ICHHI), a non-profit agency.

Since then, HMIS usage in the state has grown, with the responsibility for actual management of the effort transferring to the Indiana Housing and Community Development Authority (IHCDA) in March, 2009. At present, the HMIS effort in the Balance of State for Indiana is supported by three HUD grants to IHCDA, Evansville and South Bend. All homeless service providers have access to the same database across the state, with the exception of those in Marion County (Indianapolis.) Once responsibility for the HMIS was assumed by IHCDA, the focus of effort has been on building participation by all homeless serving agencies, with some social service and Community Action Agencies no longer using the AWARDS database. On an annual basis, IHCDA renews its contract for services and licenses with Foothold Technology. There is currently no fee for users of the HMIS, who are limited to agencies providing services to the homeless.

IHCDA maintains a staff devoted to the expansion, training and maintenance of the HMIS in Indiana. They operate a user helpline, provide various types of user training, support the local Continuums of Care, prepare the annual Point in Time Count data, develop the Annual Homeless Assessment Report (AHAR) and assist in evaluating HUD McKinney-Vento applicants. The responsibility for overall oversight of the IHCDA HMIS effort rests with the IHCDA Board, who has delegated it to the Indiana Planning Council on the Homeless and its Data Collection and Evaluation Committee. This Committee has representation from State agencies, academia, homeless service provider users of the database and advocates for the homeless.

The Data Collection and Evaluation Committee receives, reviews and makes recommendations on the basis of reports and data related to the Homeless Management Information System. This includes periodic reviews of user and executive satisfaction with the present software, discussion of changes in HUD Data Standards and opportunities to improve the system, especially with respect to greater use by non-HUD funded homeless providers. The goal for the HMIS is its statewide adoption by over 70% of all homeless shelter providers and 85% of all transitional and permanent supportive housing providers.

The AWARDS database is remotely hosted by Foothold Technology, Inc. and is operated in secure environment which requires a personally assigned log-in password to access. Each HMIS user completes a User Code of Ethics attesting to his/her awareness of the sensitivity and privacy of Protected Personal Information (PPI) and completes new user training. Only staff members with a need to know are issued log in access to the HMIS, with most being restricted to information about clients with whom they have direct contact. Additionally, each agency at which HMIS is installed completes an Agency User Agreement which specifies the privacy standards and computer safeguards expected in using the HMIS. Data integrity is assured by several levels of backup, including a separate annual archive.

Agency Participation Requirements

Policy:	IHCDA will establish requirements for Agencies that participate in the HMIS. All requirements for participation are outlined in the sections below. At present participation is limited to agencies engaged in work with the homeless, including PATH teams.

Procedure:

A. IDENTIFICATION OF AGENCY EXECUTIVE USER:

HMIS Agency Executive Users play a critical role in the protection of HMIS data. Some Agencies in our Continuum of Care have Information Technology Department Staff who could also serve as Agency System Management. Time, interest, and ability are the biggest factors in determining who should be an Agency Executive User of the HMIS. This title does not necessarily correspond to the Agency's organizational chart. The Agency User designated as the Agency Executive User may also enter Client data. The Agency Executive User shall attend training provided by IHCDA prior to performing the role. . Roles and responsibilities for the HMIS Agency Executive Users include the following:

1. Determining appropriate access to the HMIS for each Agency User. This determination should be based on each Agency User’s job function as it will relate to the HMIS data entry and retrieval (*i.e.*, role based security).
2. Detecting and responding to violations of HMIS Policies or Agency Policies and Procedures.
3. Developing strict procedures for issuing, altering and revoking access privileges.
4. Ensuring system auditing (within Agency).
5. Ensuring Agency-wide data quality.
6. Ensuring the security of the system on the Agency site.
7. Notifying IHCDA staff of any security breach within 24 hours of the breach.
8. Enforcing agency information system policies and standards.

B. TRAINING:

Agency Executive Users and designated staff persons shall attend training(s) prior to accessing the system online. If the Agency Executive User changes, the new Executive User must undergo training conducted by HMIS Staff or an individual approved by HMIS Staff. All new Agency Users of the system must undergo formal training provided by HMIS Staff or an authorized and trained individual from the Agency within 90 days of receiving an username and password. The Agency Executive User and designated staff persons will attend follow-up training provided to ensure data quality and completeness.

C. PRIVACY PRACTICES:

The ***HMIS Notice of Privacy Practices*** is designed to provide information to Clients about the ways in which their personal data may be used in the HMIS. Only staff who work directly with Clients or who have administrative responsibilities that require the use or disclosure of Client records will receive authorization to look at, enter, print, or edit Client records.

The Notice of Privacy Practices must be posted at each intake location and on the Agency's website, if applicable, to ensure the Client's knowledge of their privacy protection and rights. All staff working with the HMIS shall explain the privacy protections to Clients when asked. The Agency Executive Officer will provide annual privacy and security training to each Agency User. The current ***HMIS Notice of Privacy Practices*** will be posted at www.IHCDA.in.gov. If the Agency is a "covered entity" under the Health Insurance Portability and Accountability Act of 1996, the Agency may combine the HMIS Notice of Privacy Practices with the notice of privacy practices required by HIPAA. Agencies must request IHCDA to review any such combined Notice of Privacy Practices for compliance with HMIS and IHCDA standards. The Agency's privacy policies must meet the following requirements.

1. Collection Limitation: An Agency may collect PPI only when appropriate to the purposes for which the information is obtained or when required by law. An Agency must collect PPI by lawful and fair means and, where appropriate, with the knowledge or consent of the Client. An Agency must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information. Consent of the individual for data collection may be inferred from the circumstances of the collection. An Agency may use the following language to meet this standard: "`We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for our clients, and to better understand the needs of our clients. We only collect information that we consider to be appropriate."

2. Data Quality: PPI collected by an Agency must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PPI should be accurate, complete and timely. An agency must develop and implement a plan to dispose of or, in the alternative, to remove identifiers from, PPI that is not in current use seven years after the PPI was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention).

3. Purpose Specification and Use Limitation: An Agency must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures. An Agency may use or disclose PPI only if the use or disclosure is allowed by the Policy and Procedure on Data Use and Disclosure and is described in its privacy notice. An Agency may infer consent for all uses and disclosures specified in the notice and for uses and disclosures determined by the Agency to be compatible with those specified in the notice. Except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards, all uses and disclosures are permissive and not mandatory. Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law.

4. Openness: An Agency must publish a privacy notice describing its policies and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request. If an Agency maintains a public web page, the Agency must post the current version of its privacy notice on the web page. An Agency may, if appropriate, omit its street address from its privacy notice. An Agency must post a sign stating the availability of its privacy notice to any individual who requests a copy.

An Agency must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the Agency before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. All amendments to the privacy notice must be consistent with the requirements of these Policies and Procedures. An Agency must maintain permanent documentation of all privacy notice amendments.

5. Access and Correction: In general, an Agency must allow an individual to inspect and to have a copy of any PPI about the individual. An Agency must offer to explain any information that the individual may not understand.

An Agency must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual. In its privacy notice, an Agency may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PPI:

a. Information compiled in reasonable anticipation of litigation or comparable proceedings;

b. Information about another individual (other than a health care or homeless provider);

c. Information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or

d. Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

An Agency can reject repeated or harassing requests for access or correction. An Agency that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

Prior to agreeing to grant an individual a right to access or correct, an Agency shall consult with IHCDA to ensure that the proper coordination between the Agency's response and the capabilities of the HMIS system will occur, unless the requested correction is a routine correction of a common data element for which a field exists in HMIS (*e.g.*, date of birth, prior residence, social security number, etc.).

6. Accountability: An Agency must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. Each Agency shall forward any complaints regarding the use or disclosure of Client information by or through the HMIS for IHCDA's evaluation of the complaint. An Agency must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) the ***HMIS User Code of Ethics*** that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

D. CLIENT CONSENT FORMS:

The Indiana HMIS allows implied consent for the sharing of information provided the Notice of Privacy Practices is prominently posted. Client Consent Forms must be easily available to all clients to authorize limitations on the sharing of their Personal Information on paper or electronically with other participating Agencies through the HMIS where applicable. The HMIS presents a form for Consent. This should be filled in to allow sharing unless the client explicitly asks for limitations on his/her data in writing by signing and indicating the type of restriction requested on the HMIS generated Consent form.

Agency policies for data sharing with other Agencies should be reviewed periodically. Appropriate safeguards will be negotiated between and among Agencies if sharing data. No identified Client records will be shared electronically with another Agency without an agreement among the sharing Agencies. Any such agreement must be reviewed and approved by IHCDA

Data Protocols:

1. All Agencies must collect the Universal Data Elements as defined by HUD. Agencies receiving certain types of funding may also be required to collect the Program Data Elements as required by HUD or IHCDA. Finally, IHCDA may identify other data elements that some or all Agencies will be required to submit.
2. This data will be accurately put into the HMIS within 14 days of data collection as provided for in the Agency Partner Agreement.
3. Agency Users shall ensure all information stored in the HMIS is completely accurate. Entry of inaccurate information in the HMIS may result in revocation of a user license or licenses.
4. If an Agency User does not have the information for a particular data field, he or she must not enter any incorrect values, but shall wait to complete the screen until answers to all data fields are known.

E. AGENCY PARTNER AGREEMENT:

The Executive Director or authorized official must sign an Agency Partner Agreement stating the Agency's commitment to adhere to the policies and procedures for effective use of the HMIS and proper collaboration with IHCDA. The current ***IHCDA HMIS Agency Partner Agreement*** is posted at www.IHCDA.in.gov.

F. ENFORCEMENT OF PROPER USE OF THE HMIS:

All Agency Users of the HMIS will sign the ***HMIS User Code of Ethics***. This form states the policy, User responsibility, and Code of Ethics each Agency User must adhere to and comply with whenever using the HMIS. Violation of this policy may be considered a violation of the Agency User's employment with the Agency, and could result in disciplinary action, up to and including termination of the Agency User's employment or affiliation with the HMIS as well as potential personal civil and criminal legal fines and penalties. The current ***HMIS User Code of Ethics*** is posted at www.IHCDA.in.gov

G. IMPLEMENTATION ASSESSMENTS

Agencies may be assessed to monitor their compliance with the procedures outlined in HUD's HMIS Data and Technical Standards and these Policies and Procedures. Agencies should conduct a self-assessment at by downloading the current ***HMIS Implementation Assessment Checklist*** at www.IHCDA.in.gov

Access Privileges to HMIS

Policy: HMIS staff and participating Agencies will apply the Agency User access privilege conventions set forth in this procedure as well as enforcing location access privileges to the system servers.

Procedure:

HMIS User Code of Ethics must be signed by all Agency staff, volunteers or consultants prior to HMIS training and issuance of passwords to the HMIS. A copy will be sent to IHCDA and will be kept on file.

User Access Privileges to HMIS

A. AGENCY USER ACCESS:

Agency User access and Agency User access levels will be determined by the executive leadership of the participating Agency in consultation with the Agency Executive Officer. HMIS Staff or the Agency Executive User will generate a username and password for the Agency User who will, in turn, then generate a unique password the first time accessing the HMIS. The Agency User will be the only person to know the unique password.

Agency Users are bound by the ***HMIS Code of Ethics*** *and the* ***IHCDA HMIS Agency Partner Agreement*** and shall comply with same. All Agency Users have a critical role in the effort to protect and maintain HMIS information systems and data. Agency Users of HMIS computing resources and data have the following responsibilities:

1. Agency workstations should be configured to automatically turn on a password protected screen saver when the workstation is temporarily not in use. Agency Users **must** log off the HMIS or lock their workstation when leaving their work station **AND** close the Internet browser to prevent someone from viewing the last Client screen.
2. Read and sign the ***HMIS Code of Ethics*** when joining an Agency and every three years thereafter.
3. Support compliance with all federal and state statutes and regulations.
4. Maintain the confidentiality of sensitive information to which they are given access privileges.
5. Accept accountability for all activities associated with the use of their Agency User accounts and related access privileges.
6. Report all suspected security and/or policy violations to an appropriate authority at the Agency (*e.g.*, manager, supervisor, system administrator or the HMIS Security Officer).
7. Follow all specific policies, guidelines and procedures established by the Agencies with which they are associated and that have provided them access privileges.

Violators of this policy may be denied access to HMIS computing and network resources and may be subject to other penalties and disciplinary action within and outside of their Agency. Documented procedures should be in place for issuing, altering, and revoking access privileges on shared systems. Agency Users' access rights to HMIS shall be in the sole discretion of IHCDA.

B. IHCDA User Access:

Only IHCDA staff with a need to access the HMIS Client database shall be given access rights. Prior to being given access rights, they shall be trained on HMIS privacy and security policies and sign a HMIS Code of Ethics as herein.

C. Passwords:

1. An Agency will permit access to HMIS only with use of an Agency User authentication system consisting of a username and a password which the Agency User may not share with others. Temporary passwords are created when a new Agency User is created.
2. The Agency User will be required to change the password the first time they log onto the system. Passwords are the individual's responsibility and Agency Users cannot share passwords and should be securely stored and inaccessible to other persons. Passwords should never be stored or displayed in any publicly accessible location. Passwords should be designed to prevent individual Agency Users from being able to log onto more than one workstation at a time, and to prevent Agency Users from being able to log onto the network at more than one location at a time.
3. The password must be between 8 and 12 characters and contain a mix of alpha and numerical characters (alphanumeric). Passwords should not use or include the Agency User's username, the HMIS name, the Agency's name, or IHCDA's name. Passwords should not be easily guessed or found in any dictionary (spelled in correct or reverse order).
4. Passwords should be changed periodically by each Agency User. IHCDA requires that HMIS passwords are changed at least every 90 days.
   a. The Agency Executive User must immediately notify IHCDA staff of the Agency User's termination to allow IHCDA staff to terminate the Agency User's access rights. If a staff person is to go on leave for a period of longer than 45 (forty-five) days, their password should be inactivated immediately upon the start of their leave. It shall be the responsibility of the Agency Executive Officer to routinely ensure that usernames and passwords are current and to immediately notify IHCDA staff in the event that usernames and passwords are not current.

D. Electronic Transmission of User identification and passwords:

No one shall engage in electronic transmission of Agency User ID's and passwords, including temporary passwords, without the approval of IHCDA. Authenticators will be transmitted only by surface mail, phone, or in person unless otherwise approved by IHCDA.

E. Tracking of unauthorized access:

IHCDA will periodically review all HMIS and HMIS vendor security logs, including, where available, the transactions log, the internet log, the log of web server errors, the firewall log, tracking attempts at unauthorized access at the direction of the HMIS Security Officer. The HMIS vendor shall establish attempt thresholds to ensure HMIS security. IHCDA will follow up with Agencies at which the logs reveal questionable activity and may require corrective action to be taken by any such Agency.

Security

Policy: Access to all computing, data communications and sensitive data resources will be controlled. Access is controlled through user identification and authentication. Agency Users are responsible and accountable for work done under their username. Access control violations must be monitored, reported and resolved. Agency staff will work to ensure that all sites receive the security benefits of the system while complying with all HMIS policies

Procedures:

To protect the availability, security, and integrity of the HMIS, all computing systems (including, without limitation, networks, desktops, laptops, mini-computers, mainframes, and servers) accessing the HMIS or containing personal protected information shall comply with the minimum security measures and practices outlined herein. HMIS User agencies are not to maintain HMIS data files on their own computers and/or servers, with the exception of formatted reports and other aggregate data without PPI. Foothold Technology and IHCDA maintain fully compliant secure databases which allow 24 hour access to all qualified users. Agencies shall develop and enforce policies and procedures to address the following areas of data security and integrity:

A. PHYSICAL SECURITY:

In order to ensure that unauthorized persons cannot physically access servers, physical security measures and objectives will be implemented where applicable and appropriate to protect HMIS computing and network assets. As with logical security measures at IHCDA, physical security measures required for protecting the HMIS computing resources shall be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved. The more sensitive and critical the computing environment, the more control measures are likely to be needed. Because the system will be collecting and storing sensitive information, physical access control measures sufficient to prevent the HMIS from unnecessary and unauthorized access, use, misuse, vandalism, or theft will be implemented. All specific tools, systems, or procedures implemented to meet physical security requirements should be selected on the basis of its cost-effectiveness and common sense.

IHCDA shall ensure that the HMIS application vendor and data custodian provides the following security, as well as follows all other security measures set forth in this Policy and Procedure:

1. HMIS data shall be copied on a regular basis to another medium (*e.g.*, tape) and stored in a secure off-site location.
2. Off-site storage shall include fire and water protection for the storage medium.
3. Surge suppressors shall protect physical systems for collecting and storing the HMIS data.
4. Central server, mainframe or mini-computer shall store the central hardware in a secure room with an uninterrupted power supply, a raised floor, and appropriate temperature control and fire suppression systems.
5. Electronic data transmission transmitted over publicly accessible networks or phone lines shall be encrypted to at least 128-bit encryption.
6. Electronic data shall be stored in a binary, not text, format. Protected Personal Information shall be stored in an encrypted format using at least a 128-bit key.

7. Access to the physical system shall be controlled.
8. Network redundancy built into central server site and/or alternate site..
9. Staff on site or on call 24x7.
10. Server firewall and virus protection shall be maintained and kept current.

B. User Security

Agencies shall address the following areas:

1. Agency User Access: Agency Users will only be able to view the data entered by Agency Users of their own Agencies or shared Client records. Security measures exist within the HMIS which restrict Agencies from viewing others data unless Client consent for sharing has been obtained.
2. Agency Policies Restricting Access to Data: Each Agency must establish internal access to data protocols. These policies should include who has access, for what purpose, and how they can transmit this information. Other issues to be addressed include storage, transmission and disposal of these data. Agencies must have written policies and procedures in place regarding the appropriate access of Client data in the HMIS and its obligations under this Policy and the Agency Partner Agreement. The policies must include, without limitation, when, where and under what circumstances it is deemed appropriate for Agency staff to access HMIS data outside the office. The policies must also indicate the consequences for staff failure to abide by the policies.
3. Raw Data: Agency Users who have been granted access to the HMIS report functionality have the ability to download and save Client level data onto their local computer. Once this information has been downloaded from the HMIS in raw format to an Agency's computer, these data then become the responsibility of the Agency. An Agency must develop a protocol regarding the handling of data downloaded from the report writer, record disclosure and storage.
4. The HMIS software will automatically log off after a pre-set interval of inactivity.

C. Media and Hardcopy Protection:

The Agency must secure any electronic media or hard copy containing identifying information that is generated either by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms. Any paper or other hard copy generated by or for the HMIS that contains identifying information must be supervised at all times when it is in a public area. If Agency staff is not present, the information must be secured in areas that are not publicly accessible in a secure manner (*e.g.*, locked filing cabinet or locked office). Agencies wishing to dispose of hard copies containing identifying information must do so by shredding the documents or by other equivalent means with approval by IHCDA. In addition, in order to delete data from a data storage medium, the Agency must have procedures that require the reformatting of the storage medium. The data storage medium should be reformatted more than once before reusing or disposing of the medium.

D. Agency User Authentication:

Authorization is the provision of specific permissions or authority to have access. Access control measures required for establishing Agency Users’ access to any HMIS computing resources shall be commensurate with the functional nature and degree of criticality of the computer systems, network resources, and data involved. All Agency Users' system access will be based on the "principle of least privilege" and the "principle of separation of duties."

There will be multiple levels of access to the HMIS. The appropriate access to the HMIS is determined for each Agency User. This determination is to be based on each Agency User's job function as it will relate to the HMIS data entry and retrieval and will be officially designated by the Agency Executive Officer.

The HMIS will only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent theft. .

E. CONFIDENTIALITY

Confidentiality ensures the level of privacy of specific information. The HMIS application provides for this by encrypting the data sent over the internet. In addition, every effort must be made through policies to ensure that any personal identifiable data entered remains so, especially at the intake point.

Any staff, volunteer or other person who has been granted an Agency User ID and password and is found to have committed a breach of system security and/or Client confidentiality may be subject to sanctions including but not limited to a warning or revocation of HMIS access rights. A revoked Agency User may be subject to discipline by the Agency pursuant to the Agency's personnel policies.

Federal, state and local laws seek to protect the privacy of persons with physical and/or mental illness, who have been treated for alcohol and/or substance abuse, have been diagnosed with HIV/AIDS, and/or have been a victim of domestic violence. The Agency is encouraged to seek its own legal advice in the event that a non-partner Agency requests identifying confidential Client information.

F. INTEGRITY

Integrity provides assurance of an unaltered or unmodified state of information. All systems are required to have the capability to log basic information about Agency User access activity and for the possible creation of historical logs and access violation reports. Persons with Agency Executive User access must be able to audit Agency User activity by Agency User ID, time, date and what Client records were added, changed or deleted. The Agency Executive User should review audit reports periodically to ensure appropriate privacy and data access policies are being followed. Deviations from policy should be reported to IHCDA at within twenty-four hours of discovering the inappropriate access.

G. AVAILABILITY

Availability ensures that there is no delay or denial of authorized services or loss of data processing capabilities. This takes into account things such as virus protection, firewalls, intrusion detection, management of operating system updates, backup and recovery, and physical security to make sure that the application and database are available for the Agencies to use.

H. COMPUTER OPERATING SYSTEM MAINTENANCE

Plans must be in place to keep the computers used to access the application updated with the latest security and other updates for the operating system.

I. **Firewalls and Virus Protection**

Each Agency will have firewall protection on its networks or computers providing a barrier between the organization and any systems, including the Internet and other computer networks, located outside of the organization accessing the internet and the application. For example, a workstation that accesses the Internet directly through a modem would need a firewall; however, a workstation that accesses through a central server would not need a firewall as long as the server has a firewall.

Virus protection must also be in place employing commercially available virus protection software that includes automated scanning of files as they are accessed by Agency Users on the system where the HMIS application is housed. Each Agency and IHCDA must also subscribe to virus software, as well as an updates subscription to maintain the virus definitions and code base.

J. **Personnel Security Measures**

All HMIS Agencies will establish and maintain all necessary processes and procedures to properly and immediately close and remove all system and network privileges and resources when an employee is terminated including notifying IHCDA to disable the account~~.~~

K. **Disaster Protection and Recovery**

The HMIS is redundant and physically backed up by the vendor in accord with all current HUD requirements. It is recommended that larger agencies consider their own back up of any HMIS data maintained on site. All HMIS agencies should have a disaster plan that allows uninterrupted business access to the internet for the purposes of the HMIS despite fire, flood or other disaster.

Agency Implementation Assessments and Denial of User or Participating Agency Access

Policy: A participating Agency or Agency User's access may be suspended or revoked for suspected or actual violation of the privacy or security protocols. HMIS and IHCDA Community Services Staff, under the direction of the HMIS Program Manager and/or Data Quality Manager shall perform random Implementation Assessments of Agencies. Serious or repeated violation by Agency Users of the system may result in the suspension or revocation of an Agency's access.

Procedure:

A. AGENCY RESPONSIBILITY

1. Agencies are responsible for understanding and ensuring that their Agency Users abide by the following policies posted on www.IHCDA.in.gov.
   a. HMIS User Code of Ethics;
   b. HMIS Notice of Privacy Practices;
   c. These Policies and Standard Operating Procedures;
   d. IHCDA HMIS Agency Partner Agreement; and
   e. Any other policies or procedures issued by IHCDA.
2. Agencies shall pass the Implementation Assessments performed by HMIS staff or perform remedial actions required to pass the Implementation Assessment within the time period provided by HMIS staff.
3. Agencies may self-assess by downloading the current HMIS Implementation Assessment Checklist on www.IHCDA.in.gov.

B. IHCDA STAFF PROCEDURE:

1. IHCDA staff shall perform random Implementation Assessments following the Implementation Assessment Checklist. These assessments may occur in conjunction with other monitoring or inspections performed by IHCDA staff that is not specific to the HMIS.
2. IHCDA Staff shall call the Agency Administrator to arrange a time to meet. If the Agency Administrator is not available, another Agency staff member familiar with the HMIS operation should accompany the HMIS staff member during the Implementation Assessment.
3. Violations of security or privacy protocols will be investigated by the Agency and HMIS staff.
4. All confirmed violations of a breach of a Client's Personal Information will be communicated in writing by the Agency to the affected Client within 14 days, unless the Client cannot be located. If the Client cannot be located, a written description of the violation and efforts to locate the Client will be prepared by the Agency, and placed on file in the IHCDA office files and the Client file at the Agency.

5. If the Agency failed the Assessment and follow up work is required, the proposed next Implementation Assessment date will be negotiated, with the necessary corrective actions completed prior to the next Implementation Assessment.
6. Any Agency User found to be in violation of security protocols may be sanctioned accordingly. Sanctions may include but are not limited to: submission of a plan of correction, a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of the Agency Partner Agreement, and civil or criminal prosecution.
7. All sanctions are imposed by IHCDA.
8. All sanctions can be appealed to the Data Collection and Evaluation Committee for a non-binding advisory opinion on whether the sanction is appropriate. In all cases, IHCDA retains the final discretion and authority to impose sanctions.
9. Additional sanctions may be imposed by funders.
10. The existence of this Policy and the conduct of periodic Implementation Assessments does not preclude IHCDA from taking action if an Agency commits a violation of these Policies and Standard Operating Procedures, the Agency Partner Agreement, or the other IHCDA or HMIS policies and such violation is discovered by IHCDA through other means.

HMIS Training

Policy:	HMIS Staff will administer training to new and existing Agency Users including pre-training contact, advanced webinar instruction, and post-training follow up.

Procedure:

HMIS Staff are the primary responsible party for training Agency Users. The training administered by HMIS staff is a required activity by all HMIS users at least annually, as verified by registration for and attendance at a scheduled webinar training hosted by IHCDA. Training webinars are offered on a variety of topics and to an audience from new users through advanced users interested in executive level reports and/or preparation of required Annual Progress reports or other HUD required summaries. HMIS trainers include IHCDA staff, representatives of Foothold Technology and contracted consultants.

New Users: Prior to issuance of a user password each new user must complete the User Code of Ethics and return it to IHCDA, preferably via fax. Upon receipt, the HMIS staff can issue a user name and initial password. The new user is expected to attend a new user training within a short interval of receiving his/her user name and access. All users are expected to be active on the HMIS and to have attended training on an at least annual basis.

Established Users: All HMIS users are required to attend at least one training session annually. The topic of training may be chosen by the user and need not be a repeated session of new user training. Any user not completing at least one training annually after 1/1/2010 will automatically lose their user rights and be required to apply to have an HMIS user account, including having to complete new user training again.

Training: Participation in training will be evidenced by the logs maintained for on line webinars and/or sign in sheets at live trainings. Any HMIS user found to be logging in to training but not actively following the session, as evidenced by electronic monitoring of alternate key stroke activity and other open windows, will be required to repeat the training.

HMIS User License Billing

Policy: Homeless serving agencies have access to the IHCDA maintained HMIS without cost. There is no requirement that an agency receive HUD or other federal or state funds to participate. IHCDA reserves the right to charge a reasonable fee for the use of the HMIS for other purposes, e.g. the Homeless Prevention and Rapid Rehousing Program. Each agency is limited to a single license of no more than 15 users, unless special arrangements are made with IHCDA.

Procedure:

A. BILLING:

1. Billing is specific to the purposes and properties of the program. HPRP sub-recipient agencies are billed on a quarterly basis.

B. TERMINATING OF USER LICENSES:

1. Refunds or partial refunds will not be given to any Agency when a user license is terminated due to violating HMIS Policies and Procedures.
2. Refunds or partial refunds will not be given to any Agency when a user license is terminated in the middle of the twelve-month billing cycle for that license except in IHCDA's sole discretion in the case of rare and extenuating circumstances.

C. TRANSFERRING USER LICENSES:

1. Agencies may terminate one user license and add another license simultaneously without disrupting the billing cycle or incurring any additional costs. For example, if an Agency User needs to take a leave of absence, another Agency User can be added during that time period.
2. All licenses that are transferred must have a new username and password created.
3. All Agency Users that are added must sign the ***Code of Ethics*** and return a copy to IHCDA prior to receiving their username and password.
4. All Agency Users that are added should attend HMIS training. Training may be provided onsite by qualified Agency personnel with IHCDA's approval. Agency User may also attend a scheduled IHCDA training session.

D. CANCELLATION OF USER LICENSE:

1. Agencies may cancel a user license within 30 days of its creation, or within 30 days of receiving an invoice for a user license, at no charge.
2. Agencies that cancel user licenses may be assessed fees that have been previously waived, such as training fees and setup fees.

HMIS Technology Requests

Policy:	In order to fully participate in the HMIS, HMIS Partner Agencies may request technical assistance from IHCDA to purchase computers, manage special programs, improve internet connections, and deal with other technology items. IHCDA will establish a policy to solicit and evaluate all of these technology requests.

Procedure

A. AGENCY PROCEDURE:

1. Agency completes a Technology Request. Please submit via e-mail, the HMIS message system or telephone.
2. IHCDA reviews and considers the request. Technical requests not requiring additional funds will be evaluated by HMIS staff and responded to directly. When the request involves purchase of equipment and/or costs related to outside consultation, it will be reviewed by IHCDA on a case by case basis.
3. If the request for funding is approved, Agency may then incur the cost and/or submit documentation to IHCDA for reimbursement.
4. IHCDA reviews all requests and develops a timeline for approval and implementation.
5. Incomplete or denied requests may be resubmitted.

Data Collection and Evaluation Committee

Policy: A Data Collection and Evaluation Committee representing all Stakeholders shall be formed to regularly meet to review or create policy and resolve any issues

Responsibilities:

The Data Collection and Evaluation Committee is a committee of the Planning Council on Homelessness and, as such, advises and supports the HMIS operations in resource development, consumer involvement and quality assurance and stakeholder accountability. The Data Collection and Evaluation Committee serves as the designated authority for the HMIS to IHCDA. While the Data Collection and Evaluation Committee has responsibility for oversight, review and recommendation of the Homeless Management Information System, IHCDA is the final decision making authority on policy.

Membership Guidelines:

Membership on the Data Collection and Evaluation Committee shall be by invitation from IHCDA. The Data Collection and Evaluation Committee will be established according to the following guidelines:

1. Target membership will be 10 (ten) persons.
2. The membership shall represent the geographical mix of state-wide Agencies.
3. There will be a proactive effort to have representation from consumer representatives, shelter/transitional housing for families and individuals, other homeless services organizations and government agencies that fund homeless assistance services.
4. There will be a concerted effort to find replacement representatives when participation has been inactive or inconsistent from the organizations involved in the HMIS.
5. The term of a member of the Data Collection and Evaluation Committee shall be at the pleasure of IHCDA.

Meeting Frequency:

The committee shall meet quarterly or more frequently as needed.

Procedure

IHCDA staff shall:

1. Schedule the meeting, providing a physical and telephone location.
2. Provide administrative support for the meetings, including agenda, printing of any meeting materials and providing meeting minutes following the meeting in a timely manner.
3. Post the agenda, meeting notes and other work products from the Advisory Committee to the selected representatives of the Planning Council.

Committee shall:

1. Receive and review reports of the Homeless Management Information System.
2. Authorize and review the results of HMIS user surveys.

3. Review and approve changes necessitated by altered HUD Data Standards.

4. Periodically conduct an assessment of the present software and its vendor and make recommendations as to its continuance or change.

5. Review and approve the annual HUD NOFA application for funding, as well as the Annual Progress Report.

6. Provide expert assistance to other Planning Council Committees in support of their data driven decisions.

7. Actively explore and promote data exchange between state and other agencies toward a goal of improved service to homeless persons.

Data Use and Disclosure

Policy: The purpose of this policy is to specify how information collected by HMIS will be used or disclosed and under what conditions the information may be accessed. It categorizes the data that HMIS staff will administer and indicates the controls to ensure data integrity as information is shared.

Responsibilities:

Each of the HMIS Stakeholders has certain rights and responsibilities regarding the data collected within the HMIS.

A. HMIS SPONSORS

HMIS sponsors have rights to all De-Identified Public Data produced through the HMIS. Sponsors are:

- United States Department of Housing and Urban Development
- Indiana Housing and Community Development Authority
- Indiana Department of Education

B. HMIS STAFF

HMIS staff is responsible for the proper collection and dissemination of information among the HMIS Stakeholders. The HMIS staff is responsible for ensuring that all Client information is fully protected and that all data use conforms to IHCDA adopted policies.

C. HMIS AGENCIES AND PROGRAMS

HMIS agencies sign the ***IHCDA HMIS Agency Partner Agreement*** (posted on www.IHCDA.org) pledging their agreement and support of all policies. They also agree to post the ***HMIS Notice of Privacy Practices*** that defines the rights of Clients and contact information for the HMIS should the Client want to revoke access to their personal identified information.

Procedure:

A. ALLOWABLE USES AND DISCLOSURES OF PROTECTED PERSONAL INFORMATION ("PPI")

1. Routine Uses and Disclosures: PPI in the HMIS may be used and disclosed under the following routine circumstances:

   a. Coordination of Services: PPI may used and disclosed to provide or coordinate services to a Client.

   b. Payment: PPI may be used and disclosed for functions related to payment or reimbursement for services.

   c. Administrative Functions: PPI may be used and disclosed to carry out administrative functions, including, but not limited to legal, audit, personnel, oversight, and management functions.

   d. Creating De-Identified PPI: PPI may be used and disclosed to create De-identified Information.

2. Other Permissive Disclosures: The following additional uses and disclosures recognize those obligations to disclose PPI by balancing competing interests in a responsible

and limited way. These additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards). However, nothing in this paragraph modifies an obligation under applicable law to use or disclose PPI. The following uses and disclosures of PPI may only be made upon the approval of the Program Director:

a. Uses And Disclosures Required By Law: PPI may be used and disclosed when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.

b. Uses And Disclosures To Avert A Serious Threat To Health Or Safety: PPI may be used and disclosed, consistent with applicable law and standards of ethical conduct, if: (1) IHCDA, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

c. Uses And Disclosures About Victims Of Abuse, Neglect Or Domestic Violence: PPI about an individual whom agency staff reasonably believes to be a victim of abuse, neglect or domestic violence may be disclosed to a government authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence under any of the following circumstances:

(1) Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;

(2) If the individual agrees to the disclosure; or

(3) To the extent that the disclosure is expressly authorized by statute or regulation; and the agency believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

If such a permitted disclosure about victims of abuse, neglect or domestic violence is made, staff must promptly inform the individual that a disclosure has been or will be made, except if: (1) the Program Director, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or (2) staff would be informing a personal representative (such as a family member or friend), and the Program Director reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the Program Director, in the exercise of professional judgment.

d. Uses And Disclosures For Academic Research Purposes: PPI may be used and disclosed for academic research conducted by an individual or institution that has a formal relationship with IHCDA if the research is conducted either:

(1) By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by the Program Director (other than the individual conducting the research); or

(2) By an institution for use in a research project conducted under a written research agreement approved in writing by the Program Director.

All uses and disclosures for Research purposes shall comply with subsection E below ("IHCDA HMIS Research Policy"). Further, a written research agreement must: (1) establish rules and limitations for the processing and security of PPI in the course of the research; (2) provide for the return or proper disposal of all PPI at the conclusion of the research; (3) restrict additional use or disclosure of PPI, except where required by law; and (4) require that the recipient of data formally agree to comply with all terms and conditions of the agreement. A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

e. Disclosures For Law Enforcement Purposes: PPI may be disclosed, consistent with applicable law and standards of ethical conduct, for a law enforcement purpose to a law enforcement official under any of the following circumstances:

(1) In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;

(2) If the law enforcement official makes a written request for protected personal information that: (1) is signed by a supervisory official of the law enforcement agency seeking the PPI; (2) states that the information is relevant and material to a legitimate law enforcement investigation; (3) identifies the PPI sought; (4) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (5) states that de-identified information could not be used to accomplish the purpose of the disclosure.

(3) If IHCDA believes in good faith that the PPI constitutes evidence of criminal conduct that occurred on the premises of IHCDA or an HMIS Agency;

(4) In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics; or

(5) If (1) the official is an authorized federal official seeking PPI for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and (2) the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

B. Data Access

1. HMIS Staff: HMIS staff members may have access to all data types (including, but not limited to PPI) as necessary to perform their functions for the HMIS consistent with the Routine Uses and Disclosures listed in "A" above. HMIS staff must pass a background check and sign the ***HMIS User Code of Ethics***.
2. HMIS Sponsors' Representatives: HMIS sponsors' representatives may receive reports containing Public Data provided that representatives have applied to and have obtained written permission from HMIS staff to receive data.

3. HMIS Subcontractors and Vendors: IHMIS subcontractors and vendors have access to all data types as necessary to perform their functions for HMIS consistent with the Routine Uses and Disclosures listed in "A" above. Subcontractors and Vendors must agree in writing to maintain the confidentiality of all data received from HMIS.
4. HMIS Agencies and Programs: Agency and program staff have access to their own Agency's/program's data, as bound by these HMIS Policies and Standard Operating Procedures. Agency and program staff must sign the ***Code of Ethics*** and agree to follow these HMIS Policies and Standard Operating Procedures. HMIS Agencies and programs may also have access to Public Data and to PPI submitted by other Agencies for purposes of providing services to a Client (with Client consent).
5. Researchers: Researchers may have access to PPI and De-identified Information only in accordance with the approval procedures set forth below in "E" ("IHCDA HMIS Research Policy").
6. Other Third Parties: Data may be disclosed to other third parties (*e.g.*, media requests) only in accordance with the approval procedures set forth below in "D" ("Public Data Releases").

C. IHCDA DATA PROCESSING & PREPARATION

IHCDA may or may not do the following:

1. Cleaning: Data cleaning may be done by an HMIS Staff member, the HMIS subcontractor, or another IHCDA vendor. During this process the data is reviewed for completeness, adherence to the data schema (data types and answer ranges), and consistency with prior data releases.
2. Preparing Data: Usually some data modification is needed before it is shared. For any data that will be shared outside the Agency of origin, data preparation will include the removal of all identifying and confidential information. In addition, case filtering, data element selection or other preparation may be needed prior to data release. This is often the case when preparing data for reports or for use by analysts that are focusing on specific populations or topics. Data subsets may be extracted according to time period, Agency, Agency type or any other dimension contained within the database.
3. Data Tagging: Each data release must be accompanied by information describing the data source, time period covered, geographic area covered, and populations included. Also, any known data limitations and any context vital to accurately interpreting the data should be included.

D. PUBLIC DATA RELEASES

1. Public Data Release Procedure:

   a. HMIS Program Director Role: The HMIS Program Director shall approve or deny the general format and content of reports that contain Public Data that will be released. When a report meets the requirements of such a pre-approved format, no further HMIS Program Director approval is required. However, if a report does not meet such a pre-approved format, HMIS Program Directors approval shall be required and the HMIS Program Director shall respond to such requests for Public Data, coordinating efforts and serving as a resource to other staff and providing information to Clients regarding use and disclosure of their Protected Personal Information collected, received, used, or disclosed by the HMIS. If IHCDA administration denies an external party access to the HMIS data or adds unacceptable modifications, that party may petition the IHCDA Data Collection and Evaluation Committee to review and possibly overturn the decision. The Committee's decision shall be in its sole discretion and shall be final. The external party shall have no further right to appeal. The HMIS Program Director shall ensure that HMIS Staff maintains a log of the dates and content of any reports of Public Data that are generated and released.

b. Certify Readiness: The HMIS Program Director must approve every data or report release and must determine that the data is statistically valid for sharing. There is no one standard test; it is a judgment call made by professionally trained database specialists under management of or contracted by IHCDA. However, one statistical test might be sufficient coverage of the data subsets involved (*e.g.*, at least 60% of all data parameters). The data must meet Minimum Necessary level either pre-determined by formal thresholds, or established based on the HMIS Program Director's judgment or by the judgment of a professional data analyst hired for the purpose of certifying HMIS data. If Public Data is to be released that is not statistically valid, appropriate caveats and context must be attached to the data.

2. Types of Public Information Released: There are several types of Public Data that may be released. Information that may be released is Aggregated Data and some Client-level De-identified Information.

a. Aggregated Data

- **Pre-set Summary Reports** – simple reports of predefined information and timing released to agencies, funders' analysts, and other Stakeholders.
- **Required Reports** – including the Annual Performance Report (APR) for the U.S. Department of Housing and Urban Development and other agreed upon reports required by local funders, county, state and federal organizations.
- **Ad-Hoc Reports** – including HMIS-generated reports such as "Community Snapshots," progress reports, average length of stay reports.
- **Participation Reports** – reports that list Agencies that achieve high data entry rates, that enter data for all, some, or none of their programs, or that have data that is not of good quality. The following shall apply to Participation Reports:
  a. IHCDA will use the Housing Inventory Chart of the Continuua of Care ("CoC") in Indiana to determine the number of Emergency Shelters, Transitional Housing, and Permanent Supportive Housing programs in each CoC Region.
  b. IHCDA will publish lists of programs that are participating in the HMIS and distribute the list to local and regional CoC networks, city leaders, and other key organizations.
  c. IHCDA may publish and distribute at its discretion a list of Agencies that are entering a high level data, have data that is of excellent quality, or are using the depth and breadth of the HMIS.
  d. IHCDA may publish and distribute at its discretion a list of programs that are not entering data, have data that is of poor quality, or are not using the HMIS at all. Such reports may be statistical reports, reports of inactive logins, or other reports. Thj

b. Client-level Data

- **Data Tables** – De-identified Client-level data to be used for subsequent data analysis. Often the tables are only a selected sample (usually filtered for Client population, time period, service type or something similar) of the total cases available. Data tables are only available under the following conditions:
  a. the users are certified and pre-approved and,

b. a written request to disclose data is submitted and approved by HMIS Program Director; such requests may be on-going.

3. Release Notification: The following actions will be taken whenever HMIS generated data or report is released to the general public or to parties not directly participating in the HMIS, except for Ad-Hoc and Participation Reports as described above.

   a. In the case of released reports, identified agencies and programs will be given the opportunity to review and comment on the reports before public release.

   b. In the case of released reports, notification will be posted on the IHCDA web site at the time of release.

   c. The Data Collection and Evaluation Committee will regularly be given reports summarizing the data access requests and permissions, and the report releases.

4. IHCDA HMIS Data Release Charge: Because there are costs in generating data files or reports, IHCDA may charge external parties for the costs occurred in generating the requested data. These costs may include but are not limited to: analyst time, printing costs, and computer time, among others.

E. IHCDA HMIS RESEARCH POLICY

As a general policy, IHCDA shall not disclose Protected Personal Information for Research purposes. Upon receipt of a request for Protected Personal Information for Research purposes, HMIS Staff may provide the requesting person or entity with De-Identified Information that will allow the requestor to identify cohorts of Research subjects at individual Agencies. The requestor may then contact individual Agencies to request Protected Personal Information for purposes of the Research Activity. Notwithstanding the foregoing, the Personal Protected Information may be disclosed by HMIS Staff for Research activities pursuant to the following procedures:

1. Access to Data: External parties must apply and have written permission from IHCDA administration prior to the start of Research activity involving Protected Personal Information or De-identified Client Information. The IHCDA Program Manager and Data Analyst will generally make the determination on data access.

   a. Approval will be conditioned upon the researcher presenting an application that contains the following information:

      (1) Which Agency or organization is seeking the data;

      (2) Who the lead researcher or analyst will be;

      (3) The intended uses of the data;

      (4) An explanation as to how the Research is likely to bring benefits to the homeless service system, homeless service agencies involved, and/or directly to homeless persons;

      (5) The data elements desired, programs or components of the continuum of care to be included, and the time period covered;

      (6) A plan to provide for the security of the data in the course of the research;

      (7) A plan to provide for the return or proper disposal of all data at the conclusion of the research;

      (8) A plan to restrict additional uses or disclosures of the data (except where required by law); and

(9) A statement of the applicant's willingness to sign a written agreement containing the foregoing elements.

b. Conditions:

(1) Partner Agencies will be notified if Agency identified specific data is being provided to researchers or other external parties.

(2) Official requests for information will be handled strictly in compliance with relevant statutes and regulations. IHCDA administration will consult with the Data Collection and Evaluation Committee to acquire Stakeholder perspective.

(3) IHCDA administration may approve data access but with modifications. That is, some changes may be made, for example, to the range of accessible data, the schedule for production of that data or who from the external party may have access to the data.

(4) If IHCDA administration denies an external party access to the HMIS data or adds unacceptable modifications, that party may petition the IHCDA Executive Committee to review and possibly overturn the decision. The Executive Committee's decision shall be in its sole discretion and shall be final. The external party shall have no further right to appeal.

(5) If a researcher has obtained approval to conduct Research and later determines information is needed that differs from what was originally authorized, the Data Collection and Evaluation Committee approval process must be repeated.

c. The data elements the researcher requires will determine how they gain access to Protected Personal Information. If the elements needed meet the definition of Protected Personal Information, then the researcher has two options:

(1) **Client Authorization from the Client or their legal representative**: The authorization must contain certain elements in order to accommodate the request.

(2) **Institutional Review Board (IRB) Waiver**: A waiver of the Client authorization requirement is obtained from a recognized IRB.

If the information being requested is De-identified Information, then neither Client authorization, nor an IRB waiver is required; however, IHCDA administration approval shall still be required. It shall be the sole responsibility of the requesting researcher to obtain either Client authorization or an IRB waiver. It shall not be the responsibility of IHCDA or the Data Collection and Evaluation Board to obtain Client authorization or an IRB waiver.

2. Research Recruitment: Methods for obtaining Research subjects for a study must be approved in advance by the Data Collection and Evaluation Committee and will conform to legal and regulatory guidelines. When an approved study makes a change in their recruiting practice, the Data Collection and Evaluation Committee must re-approve the method before it is put into practice.

3. The Data Collection and Evaluation Committee Role: The Data Collection and Evaluation Committee is not a Privacy Board, nor is it an Institutional Review Board (IRB). The Data Collection and Evaluation Committee is responsible for:

a. Coordinating and monitoring Research activities that are conducted on the HMIS data. Any Research activity, regardless of funding source or original intent (*e.g.*, the activity may have started out as something else) is subject to Data Collection and Evaluation Committee oversight.

b. Providing an internal administrative feasibility review to assess: (a) the impact of Research on IHCDA staff, Partner Agencies or programs, IHCDA Clients; (b) the impact of Research outcomes;, and (c) the quality of Research design if applicable. Research must be likely to bring benefits to the homeless service system, homeless service agencies involved, and/or directly to homeless people. The Data Collection and Evaluation Committee makes the final determination whether the Research request will be granted. The Data Collection and Evaluation Committee may from time to time adapt more specific criteria for evaluating Research requests.

c. Ensuring Client privacy rights are protected as it relates to Research or Research-related activities.

.

d. Maintaining documentation related to these activities in accordance with legal regulations, regardless of funding source or IRB approvals.

e. Clarifying activities (surveillance, program evaluation/quality improvement) that may contain elements of Research.

f. Referring cases of suspected misconduct to IHCDA Executive Committee.

g. Overseeing consent process for Research subjects who would be involved in on-going Research studies. It may be combined with an authorization. It must:

(1) Describe the study

(2) Describe its anticipated outcomes and benefits

(3) Describe how the confidentiality of records will be protected.

(4) Notify the Client if photographs will be used and the purpose of the photographs

4. Charges: Because there are costs in generating data files or reports, IHCDA administration may charge external parties for the costs occurred in generating the requested data. These costs will include but are not limited to : analyst time, printing costs, and computer time, among others. Applicable charges shall be in the sole discretion of IHCDA.

Data Integration and Legacy Data Migration

Policy: IHCDA recognizes that some Agencies may want to keep their existing database and import their data periodically into the HMIS. Further, Agencies may move legacy data into the HMIS from the existing databases. This data integration/migration is allowed, provided the data integrated is accurate and meets the technical specifications set forth by the HMIS Vendor. A cost may be incurred by the Agency.

Procedure:

A. DATA INTEGRATION

Agencies who are going to import data into the HMIS will be considered full HMIS Partner Agencies and must meet all of the requirements stated in the other Policies and Standard Operating Procedures.

1. Agencies wishing to integrate data must contact IHCDA and describe the type of data, the amount of data proposed to be integrated, and the existing database that houses the data.
2. IHCDA will provide the Agency with an upload specification document for integration based on the Agency's request.
3. Agency shall review IHCDA's specification document and shall provide IHCDA with any supplemental information necessary based on the Agency's (and its vendors') capabilities.
4. Based on the foregoing, IHCDA shall provide Agency with an estimated cost for the integration.
5. Agency and IHCDA shall agree upon final implementation and costs.
6. All upload specifications must be met prior to the data integration.
7. Agencies will pay for the cost of any problems associated with the data integration at the standard rate charged by the HMIS software vendor.
8. Data that is integrated may be shared with other HMIS Agencies, provided the Agency has obtained appropriate consent from the Client.

B. LEGACY DATA MIGRATION

1. Agencies wishing to migrate legacy data must contact IHCDA and describe the type of data, the amount of data to be moved, and the existing database that houses the data.
2. IHCDA will provide the Agency with an upload specification document for migration based on the Agency's request.
3. Agency shall review IHCDA's specification document and shall provide IHCDA with any supplemental information necessary based on the Agency's (and its vendors') capabilities.
4. Based on the foregoing, IHCDA shall provide Agency with an estimated cost for the migration.
5. Agency and IHCDA shall agree upon final implementation and costs.
6. All upload specifications must be met prior to the legacy data migration.

7. Agency will pay for the cost of any problems associated with the legacy data migration at the standard rate charged by the HMIS software vendor.
8. All legacy data that is migrated may not be shared with other HMIS Agencies without the consent of the Client(s) to whom the data relates.
9. Legacy data that is more than twelve (12) months old should not be migrated, unless the data is part of a program that has a length of stay that is generally longer than 12 months.
10. The legacy data that is migrated should be accurate and of good quality.

Definitions for HMIS Policies and Standard Operating Procedures

Definitions: The following definitions shall be applicable for the HMIS Policies and Standard Operating Procedures.

Agency: An organization working with IHCDA signing an Agency Partner Agreement thereby agreeing to follow HMIS Policies and Standard Operating Procedures. The Agency Partner Agreement is in effect for all related programs within an Agency.

Agency Executive User: The individual at an Agency who is the chief liaison between IHCDA and the Agency and whose responsibilities are more fully described in the "Agency Participation Requirements" Policy and Standard Operating Procedure.

Agency User or User: An employee, agent, or other representative authorized by an Agency to receive an HMIS username and password.

Aggregated Data: This is data that is grouped, usually by program, but possibly across any dimension (e.g., time, county sub region, segments of Client populations, etc.). This data type precludes exploration at a Client-identified level because all Client-level information is de-identified.

Client: A person who applies for or receives services from an Agency.

Client-level Information: A set of data records that combined represent a single Client. This type of information lends itself to more in-depth data analysis. All public Client-level Information is De-identified Information.

De-identified Information: A data set or report that removes all Protected Personal Information, (*i.e.*, information that identifies the Client by name, SSN or other unique identifier).

Disclosure: The release, transfer, or provision of access to information outside the HMIS.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et. seq., and its implementing regulations (all as amended).

HMIS: Homeless Management Information System — a web based computer system managed by IHCDA staff that collects Client- identifying Confidential Information with services received and outcomes achieved by the Clients.

Institutional Review Board (IRB): A committee of individuals that ascertains and approves the acceptability of proposed Research and the use of Clients and Protected Personal Information in terms of institutional commitments and regulations, applicable law, and standards of professional conduct and practice.

Minimum Necessary: The minimum amount of Protected Personal Information needed to accomplish the purpose of a request or to assess Client eligibility to provide services to the Client.

Protected Personal Information: Any information maintained by an Agency or in HMIS about a Client or homeless individual that: (i) identifies, either directly or indirectly, a specific individual; (ii) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (iii) can be linked with other available information to identify a specific individual. The term shall include Protected Health Information. This information may include demographic or financial information about a particular Client that is obtained through one or more sources. This may include information such as name, address, social security number, income, education and housing information.

Protected Health Information: Any individually identifiable information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.

Program Specific Data Elements: Additional data elements that are specific to the services provided by the Agency to each Client. Program Data are a mix of those elements required to complete the HUD APR (Annual Progress Report) and additional elements suggested by other federal agencies, HMIS practitioners and researchers.

Public Data: De-identified Information approved for release to external parties and the public. It may be either Client-level Information or Aggregated Data.

Research: An activity is defined as research when it meets the following definition: “a systematic investigation, including Research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of Research repositories and databases for Research.” *(45 CFR, Part 46 — The Common Rule).* For purposes of this Policy, any use of Protected Personal Information for Research purposes must be for academic Research conducted by an individual or institution that has a formal relationship with IHCDA if the Research is conducted either: (1) by an individual employed by or affiliated with IHCDA for use in a research project conducted under a written research agreement approved in writing by the RARC; or (2) by an institution for use in a research project conducted under a written research agreement approved in writing by the RARC.

Stakeholders: IHCDA sponsors, participating agencies, programs, and homeless persons.

Universal Data Elements: Basic demographic data elements defined in the HUD Data Standards including those the Agency staff are responsible for entering into the HMIS:

Name
Date of Birth
Gender
Veteran Status
Prior Residence
Ethnicity & Race
Program entry date
Program exit date
Disabling Condition
Social Security Number
Zip Code last permanent address